MySQL Security: What's New & Best Practices

ORACLE

MySQL

43%

of companies have experienced a data breach in the past year.

Source: Ponemon Institute, 2014

Attackers Are Moving Faster

5 out of 6 large companies targeted by attackers in 2014. 40% increase over 2013.

60% Of all targeted attacks struck small and medium sized organizations.

24 Zero-day vulnerabilities in 2014. An all time high.

Nearly one million new threats (malware) released each day in 2014. And more sophisticated.

Source: Internet Security Threat Report 2015, Symantec

ORACLE

Database Vulnerabilities

- Poor Configurations
  - Set controls and change default setting
- Over Privileged Accounts
  - Privilege Policies
- Weak Access Control
  - Dedicated Administrative Accounts
- Weak Authentication
  - Strong Password Enforcement
- Weak Auditing
  - Compliance & Audit Policies
- Lack of Encryption
  - Data, Back, & Network Encryption
- Proper Credential or Key Management
  - Use mysql_config_editor , Key Vaults
- Unsecured Backups
  - Encrypted Backups
- No Monitoring
  - Security Monitoring, Users, Objects
- Poorly Coded Applications
  - Database Firewall

Database Attacks

- SQL Injection
  - Prevention: DB Firewall, White List, Input Validation
- Buffer Overflow
  - Prevention: Frequently apply Database Software updates, DB Firewall, White List, Input Validation
- Brute Force Attack
  - Prevention: lock out accounts after a defined number of incorrect attempts.
- Network Eavesdropping
  - Prevention: Require SSL/TLS for all Connections and Transport
- Malware
  - Prevention: Tight Access Controls, Limited Network IP access, Change default settings

Database Malicious Actions

- Information Disclosure: Obtain credit card and other personal information
  - Defense: Encryption – Data and Network, Tighter Access Controls
- Denial of Service: Run resource intensive queries
  - Defense: Resource Usage Limits – Set various limits – Max Connections, Sessions, Timeouts, …
- Elevation of Privilege: Retrieve and use administrator credentials
  - Defense: Stronger authentication, Access Controls, Auditing
- Spoofing: Retrieve and use other credentials
  - Defense: Stronger account and password policies
- Tampering: Change data in the database, Delete transaction records
  - Defense: Tighter Access Controls, Auditing, Monitoring, Backups

Regulatory Compliance

- Regulations
  - PCI – DSS: Payment Card Data
  - HIPAA: Privacy of Health Data
  - Sarbanes Oxley: Accuracy of Financial Data
  - EU Data Protection Directive: Protection of Personal Data
  - Data Protection Act (UK): Protection of Personal Data
- Requirements
  - Continuous Monitoring (Users, Schema, Backups, etc)
  - Data Protection (Encryption, Privilege Management, etc.)
  - Data Retention (Backups, User Activity, etc.)
  - Data Auditing (User activity, etc.)

PCI Security Standards Council™

HIPAA
Health Insurance Portability and Accountability Act

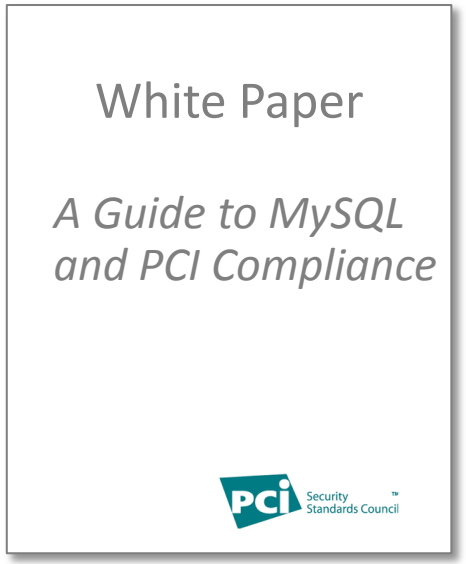
Sarbanes-Oxley
Financial and Accounting Disclosure Information

European Commission
Justice

Data Protection Act 1998

PCI-DSS

- Requirement 2: Secure Configurations, Security Settings & Patching
  - Not Using Vendor Default Passwords and Security Settings
- Requirement 3: Protecting Cardholder Data – Strong Cryptography
  - Protect Stored Cardholder Data
- Requirement 6: Up to Date Patching and Secure Systems
  - Develop and Maintain Secure Systems and Applications
- Requirement 7: User Access and Authorization
  - Restrict Access to Cardholder Data by Need to Know
- Requirement 8: Identity and Access Management
  - Identify and Authenticate Access to System Components
- Requirement 10: Monitoring, Tracking and Auditing
  - Track and Monitor Access to Cardholder Data



HIPPA

- Access Controls
  - Access only to those persons or software programs that have been granted access rights
  - Unique User Identification, Emergency Access Procedure, Automatic Logoff, Encryption and Decryption
- Authentication
  - Verify that a person or entity seeking electronic health information is the one claimed
- Integrity
  - Protect electronic protected health information from improper alteration or destruction
- Transmission Security
  - Guard against unauthorized access that is being transmitted over a network
- Encryption
  - Encrypt electronic protected health information
- Audit Control
  - Record and examine activity that contain or use electronic protected health information

Sarbanes Oxley

Sarbanes-Oxley
Financial and Accounting Disclosure Information

- Accurate and factual business and financial reports
  - Verify that the records protected from tampering and modification
- Protect data accuracy and integrity
  - Minimal permissions on data for each employee
  - Deny any privileges above minimal
  - Audit all activity

Data Protection Act – UK 1998

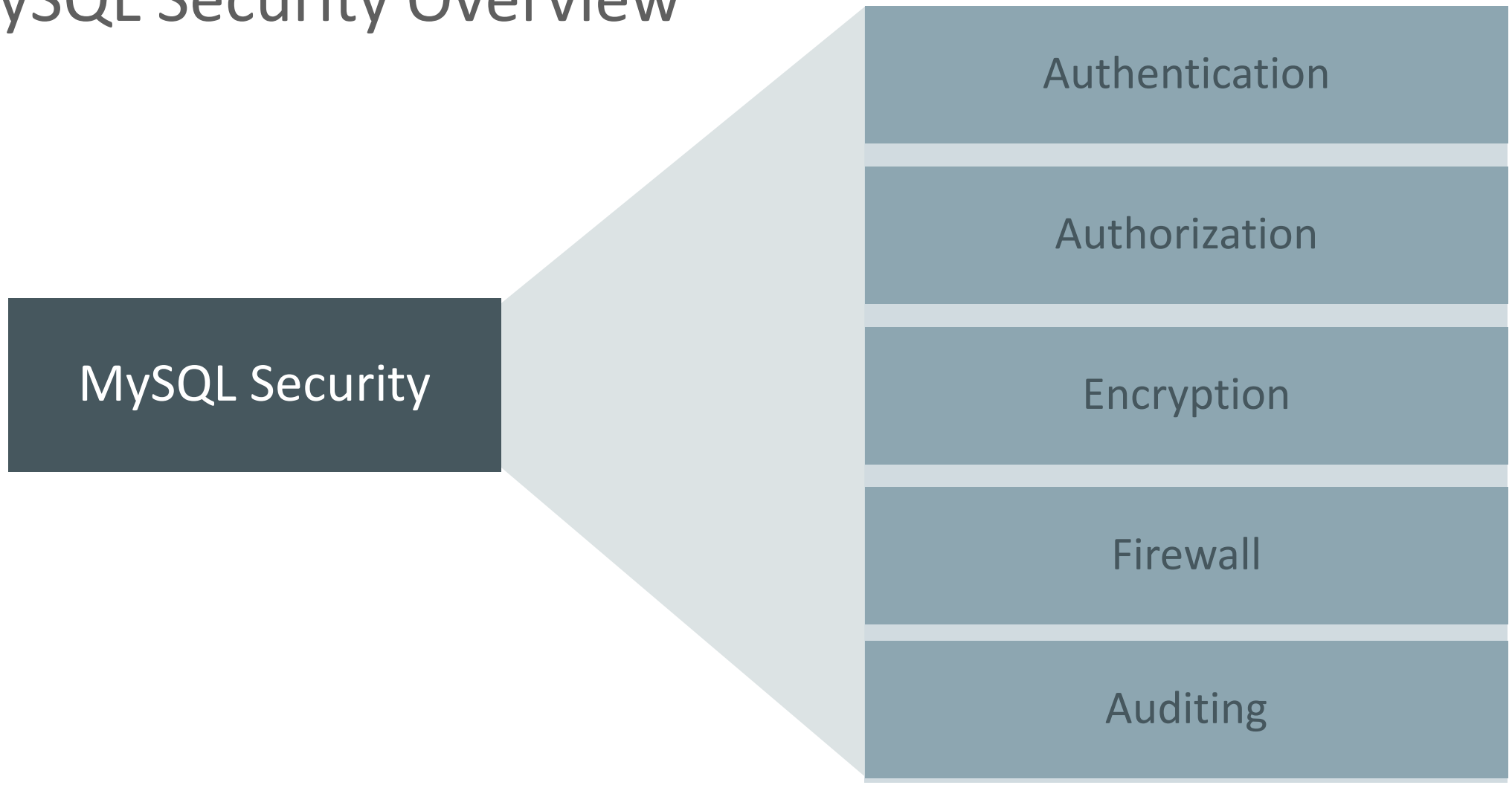
Data Protection Act 1998

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be adequate, relevant and not excessive
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data processed for any purpose shall not be kept for longer than is necessary
- Personal data shall be processed in accordance with the rights of data subjects
- Measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area

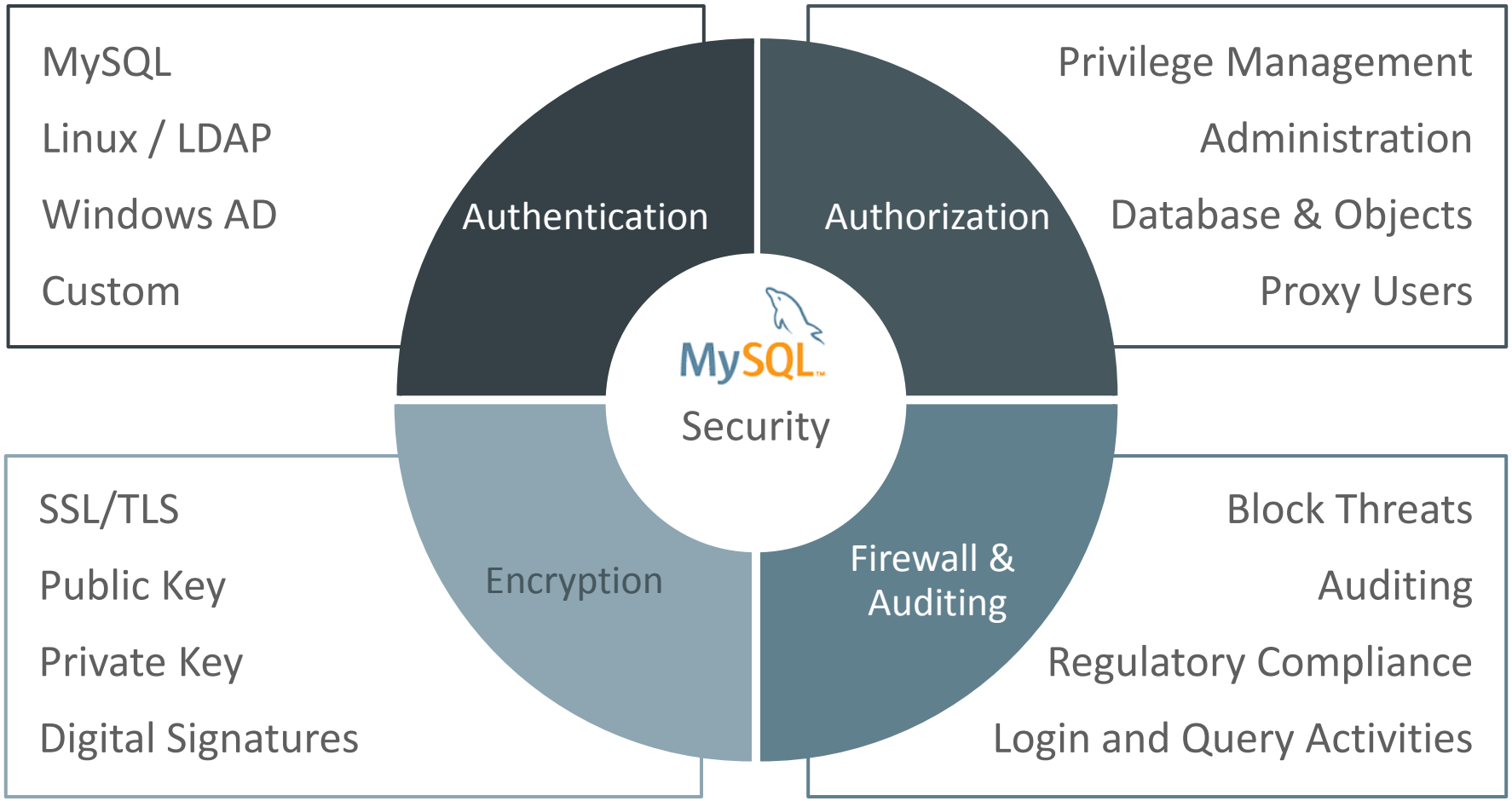
DBA Responsibilities

- Ensure only users who should get access, can get access
- Limit what users and applications can do
- Limit from where users and applications can access data
- Watch what is happening, and when it happened
- Make sure to back things up securely
- Minimize attack surface

MySQL Security Overview

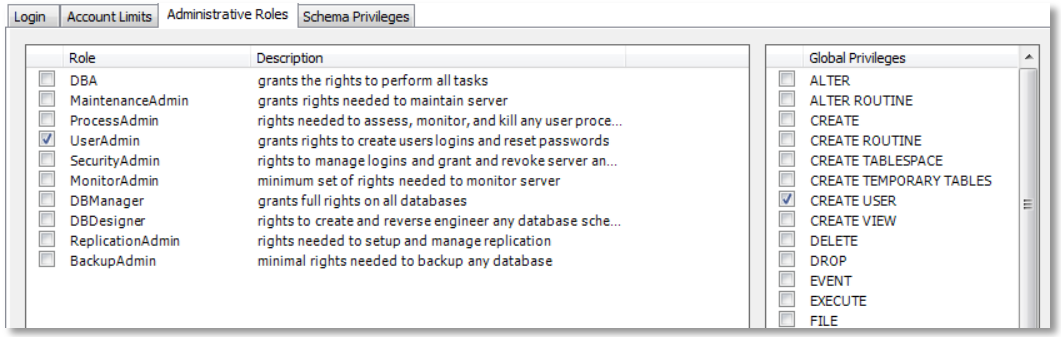


MySQL Security Overview



MySQL Authorization

- Administrative Privileges
- Database Privileges
- Session Limits and Object Privileges
- Fine grained controls over user privileges
  - Creating, altering and deleting databases
  - Creating, altering and deleting tables
  - Execute INSERT, SELECT, UPDATE, DELETE queries
  - Create, execute, or delete stored procedures and with what rights
  - Create or delete indexes



Security Privilege Management in MySQL Workbench

MySQL Privilege Management Grant Tables

user

- User Accounts
- Global Privileges

db

- Database Level Privileges
- Database, Tables, Objects
- User and host

tables_priv

- Table level privileges
- Table and columns

columns_priv

- Specific columns

procs_priv

- Stored Procedures
- Functions
- Single function privilege

proxies_priv

- Proxy Users
- Proxy Privileges

MySQL Privilege Management

- Continuous assessment
  - Configuration
  - Users
  - Permissions and Rights
- Audit & Review activity
  - Who – does activity match expectation
  - What – is this it limited as expected
  - When – acts often are at odd / off peak times
  - Where – Connections should be from expected hosts
- MySQL has simple to use controls and privileges to set secure limits

MySQL Authentication

- Built in Authentication
  - user table stores users and encrypted passwords
- X.509
  - Server authenticates client certificates
- MySQL Native, SHA 256 Password plugin
  - Native uses SHA1 or plugin with SHA-256 hashing and per user salting for user account passwords.
- MySQL Enterprise Authentication
  - Microsoft Active Directory
  - Linux PAMs (Pluggable Authentication Modules)
    - Support LDAP and more
- Custom Authentication

MySQL Password Policies

- Accounts without Passwords
  - Assign passwords to all accounts to prevent unauthorized use
- Password Validation Plugin
  - Enforce Strong Passwords
- Password Expiration/Rotation
  - Require users to reset their password
- Account lockout (in v. 5.7)

MySQL Encryption

- SSL/TLS Encryption
  - Between MySQL clients and Server
  - Replication: Between Master & Slave
- Data Encryption
  - AES Encrypt/Decrypt
- MySQL Enterprise Encryption
  - Asymmetric Encrypt/Decrypt
  - Generate Public Key and Private Keys
  - Derive Session Keys
  - Digital Signatures
- MySQL Enterprise Backup
  - AES Encrypt/Decrypt

SSL/TLS

- Encrypted connections
  - Between MySQL Client and Server
  - Replication: Between Master & Slave
- MySQL enables encryption on a per-connection basis
  - Identity verification using the X509 standard
- Specify the appropriate SSL certificate and key files
- Will work with trusted CAs (Certificate Authorities)
- Supports CRLs – Certificate Revocation Lists

Database Firewall

- SQL Injection Attacks
  - #1 Web Application Vulnerability
  - 77% of Web Sites had vulnerabilities
- MySQL Enterprise Firewall
  - Monitor database statements in real-time
  - Automatic White List “rules” generation for any application
  - Block SQL Injection Attacks
  - Intrusion Detection System

Database Auditing

- Auditing for Security & Compliance
  - FIPS, HIPAA, PCI-DSS, SOX, DISA STIG, …
- MySQL built-in logging infrastructure:
  - general log, error log
- MySQL Enterprise Audit
  - Granularity made for auditing
  - Can be modified live
  - Contains additional details
  - Compatible with Oracle Audit Vault.

MySQL Database Hardening

Installation

- Mysql_secure_installation
- Keep MySQL up to date
  - MySQL Installer for Windows
  - Yum/Apt Repository

Configuration

- Firewall
- Auditing and Logging
- Limit Network Access
- Monitor changes

User Management

- Remove Extra Accounts
- Grant Minimal Privileges
- Audit users and privileges

Passwords

- Strong Password Policy
- Hashing, Expiration
- Password Validation Plugin

Encryption

- SSL/TLS for Secure Connections
- Data Encryption (AES, RSA)

Backups

- Monitor Backups
- Encrypt Backups

ORACLE

MySQL 5.7 Linux Packages - Security Improvements

- Test/Demo database has been removed
  - Now in separate packages
- Anonymous account creation is removed.
- Creation of single root account – local host only
- Default installation ensures encrypted communication by default
  - Automatic generation of SSL/RSA Certs/Keys
    - For EE : At server startup if options Certs/Keys were not set
    - For CE : Through new mysql_ssl_rsa_setup utility
- Automatic detection of SSL Certs/Keys
- Client attempts secure TLS connection by default
- Compile time restriction over location used for data import/export operations
- Ensures location has restricted access
- Only mysql user and group
- Supports disabling data import/export
  - Set secure-file-priv to empty string

MySQL Installer for Windows includes various Security Setup and Hardening Steps

MySQL Database Hardening: Installation

- MySQL_Secure_Installation / MySQL Installer for Windows
  - Set a **strong** password for root account
  - Remove root accounts that are accessible from outside the local host
  - Remove anonymous-user accounts
  - Remove the test database
    - Which by default can be accessed by all users
    - Including Anonymous Users
- Keep MySQL up to date
  - Repos – YUM/APT/SUSE
  - MySQL Installer for Windows

Software Updates - Database and OS Maintenance

- Maintaining security requires keeping Operating System and MySQL security patches up to date.
  - May require a restart (mysql or operating system) to take effect.
- To enable seamless upgrades consider MySQL Replication
  - Allows for changes to be performed in a rolling fashion
    - Best practice to upgrade slaves first
  - MySQL 5.6 and above supports GTID-based replication
    - Provides for simple rolling upgrades
- Follow OS vendor specific hardening Guidelines
  - For example
    - http://www.oracle.com/technetwork/articles/servers-storage-admin/tips-harden-oracle-linux-1695888.html

MySQL Database Hardening: Configuration

- Audit Activity
  - *Use Enterprise Audit*
  - *Alt. Transiently enable Query Logging*
  - Monitor and Inspect regularly
- Disable or Limit Remote Access
  - If local “skip-networking” or bind-address=127.0.0.1
  - If Remote access then limit hosts/IP
- Consider changing default port
- Change root username
- Disable unauthorized reading from local files
  - Disable LOAD DATA LOCAL INFILE
- Run MySQL on non default port
  - More difficult to find database
- Limit MySQL OS User
- Ensure secure-auth is enabled

MySQL Database Hardening: Best Practices

Parameter	Recommended Value	Why
Secure_file_priv	A Designated Leaf directory for data loads	Only allows file to be loaded from a specific location. Limits use of MySQL to get data from across the OS
Symbolic_links	Boolean – NO	Prevents redirection into less secure filesystem directories
Default-storage_engine	InnoDB	Ensures transactions commits, ???
General-log	Boolean – OFF	Should only be used for debugging – off otherwise
Log-raw	Default - OFF	Should only be used for debugging – off otherwise
Skip-networking or bind-address	ON 127.0.0.1	If all local, then block network connections or limit to the local host.
SSL options	Set valid values	Should encrypt network communication

MySQL Database Hardening: Password Policies

- Enforce Strong Password Policies
- Password Hashing
- Password Expiration
- Password Validation Plugin
- Authentication Plugin
  - Inherits the password policies from the component
  - LDAP, Windows Active Directory, etc.
- Disable accounts when not in use
  - Account lockout (5.7+)

MySQL Database Hardening: Encryption

- Encryted Communication and More
- SSL/TLS encrypted for transport
- X.509 adds additional “Factor” – something you have – in addition to username/password or other authentication
  - Assures the client is validated – thus more likely trusted
- Use database and application level encryption of highly sensitive data
- User database or application functions to mask or de-identify data
  - Personal IDs, Credit Cards, …
- Consider Public Keys for Applications that encrypt only

MySQL Database Hardening: Backups

- Backups are Business Critical
  - Used to restore after attack
  - Migrate, move or clone server
  - Part of Audit Trail
- Regularly Scheduled Backups
- Monitor Backups
- Encrypt Backups

Applications and Credentials - Best Practices

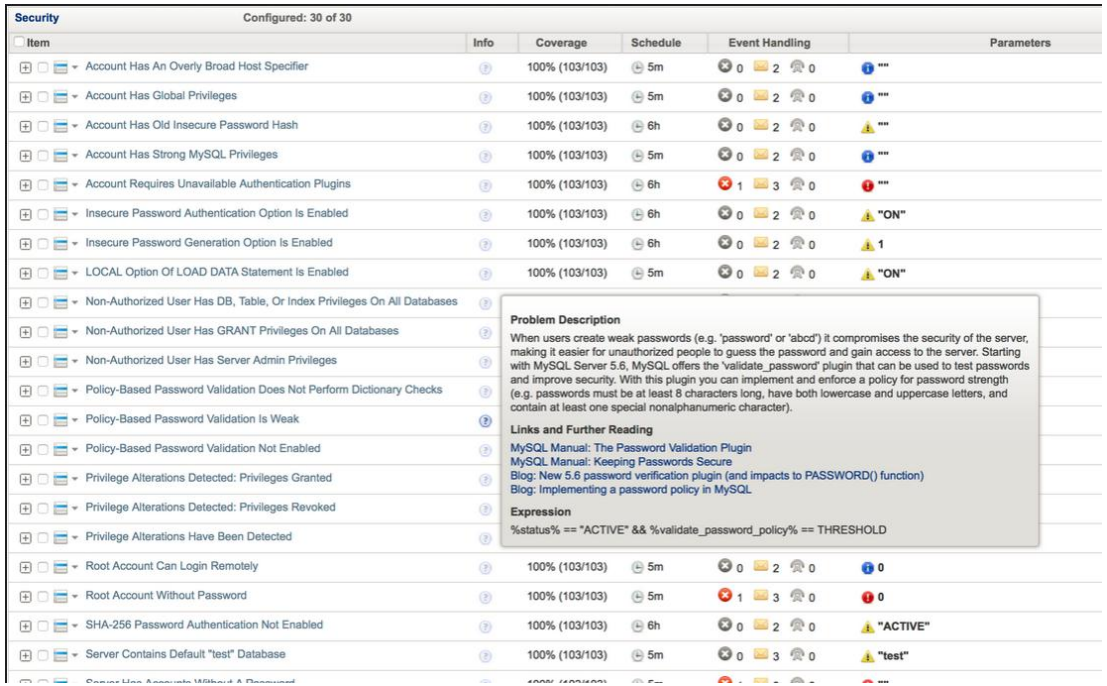
- Applications – minimize sharing a credentials (username/password)
  - Finer grained the better – don't overload across many applications/servers
- Should enable support for credential rotation
  - Do not require all passwords to be changed in synchronization.
  - Facilitates better troubleshooting and root-cause analysis.
- Steps to changing credentials should be secure and straightforward
  - Not embedded in your code
    - Can be changed without redeploying an application
    - Should never be stored in version control and must differ between environments.
    - Applications should get credentials using a secure configuration methodology.

MySQL Enterprise Edition

- MySQL Enterprise Authentication
  - External Authentication Modules
    - Microsoft AD, Linux PAMs
- MySQL Enterprise Encryption
  - Public/Private Key Cryptography
  - Asymmetric Encryption
  - Digital Signatures, Data Validation
- MySQL Enterprise Firewall
  - Block SQL Injection Attacks
  - Intrusion Detection
- MySQL Enterprise Audit
  - User Activity Auditing, Regulatory Compliance
- MySQL Enterprise Monitor
  - Changes in Database Configurations, Users Permissions, Database Schema, Passwords
- MySQL Enterprise Backup
  - Securing Backups, AES 256 encryption

MySQL Enterprise Monitor

- Enforce MySQL Security Best Practices
  - Identifies Vulnerabilties
  - Assesses current setup against security hardening policies
- Monitoring & Alerting
  - User Monitoring
  - Password Monitoring
  - Schema Change Monitoring
  - Backup Monitoring
  - Configuration Management
  - Configuration Tuning Advice
- Centralized User Management

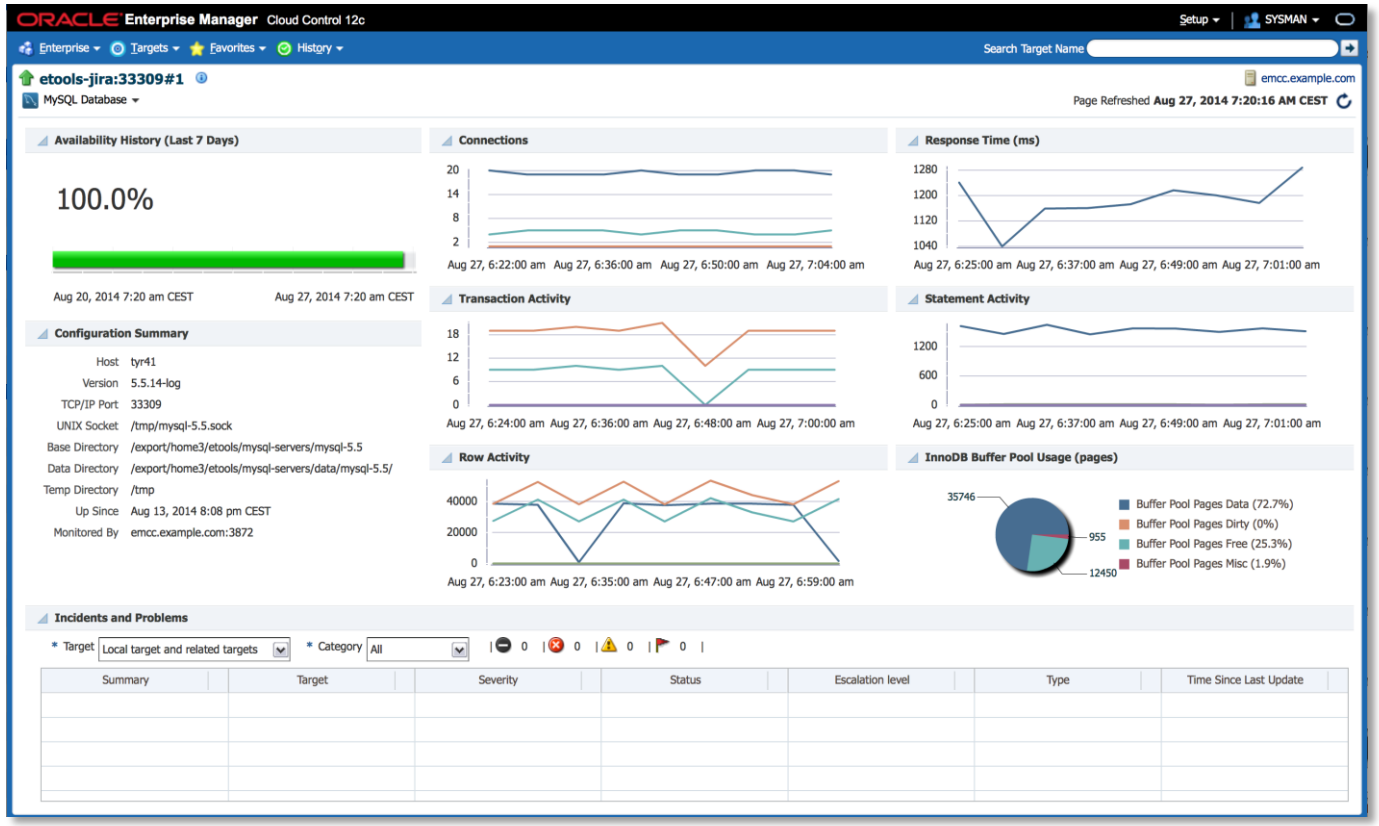


"I definitely recommend the MySQL Enterprise Monitor to DBAs who don't have a ton of MySQL experience. It makes monitoring MySQL security, performance and availability very easy to understand and to act on."

Sandi Barr
Sr. Software Engineer
Schneider Electric

Oracle Enterprise Manager for MySQL

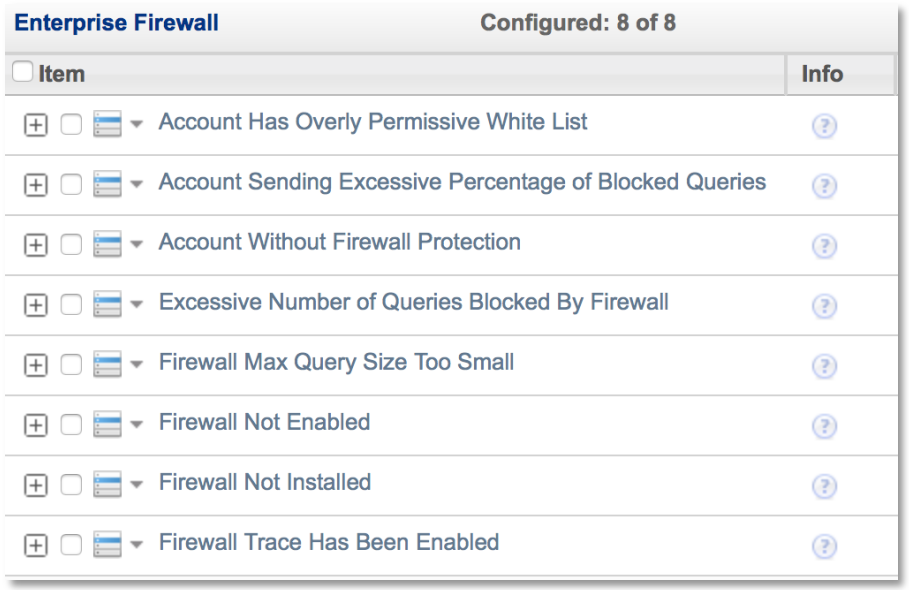
- Availability monitoring
- Performance monitoring
- Configuration monitoring
- All available metrics collected
  - Allowing for custom threshold based incident reports
- MySQL auto-detection



ORACLE ENTERPRISE MANAGER

MySQL Enterprise Firewall

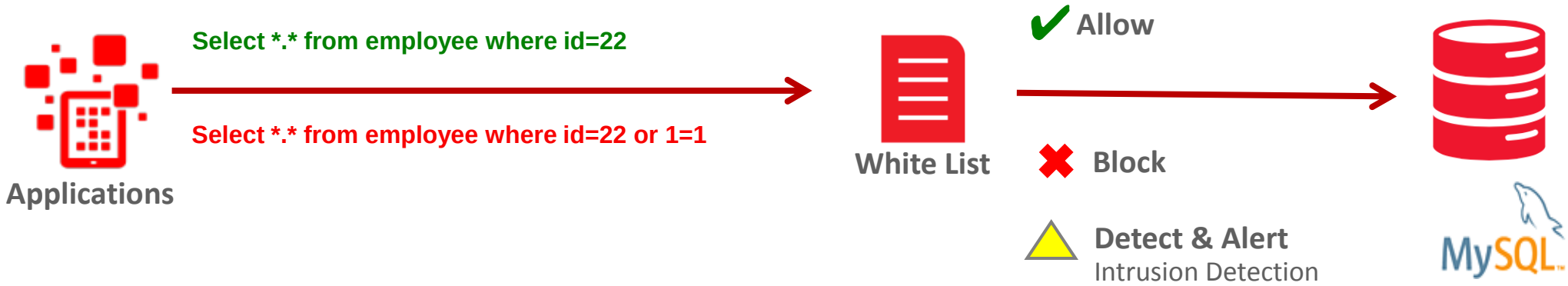
- Real Time Protection
  - Queries analyzed and matched against White List
- Blocks SQL Injection Attacks
  - Block Out of Policy Transactions
- Intrusion Detection
  - Detect and Alert on Out of Policy Transactions
- Learns White List
  - Automated creation of approved list of SQL command patterns on a per user basis
- Transparent
  - No changes to application required



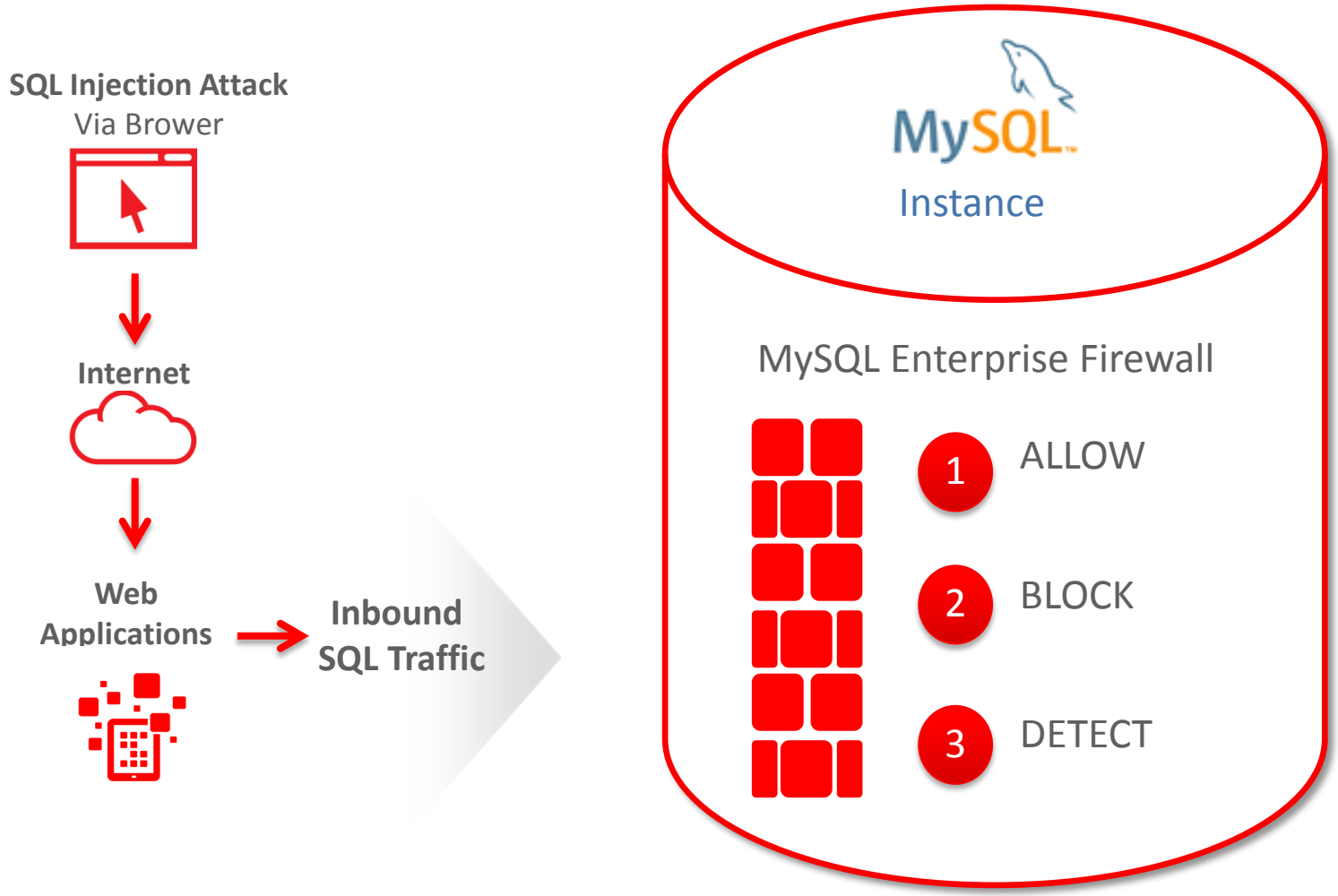
MySQL Enterprise Firewall monitoring

MySQL Enterprise Firewall

- Block SQL Injection Attacks
  - Allow: SQL Statements that match Whitelist
  - Block: SQL statements that are not on Whitelist
- Intrusion Detection System
  - Detect: SQL statements that are not on Whitelist
    - SQL Statements execute and alert administrators

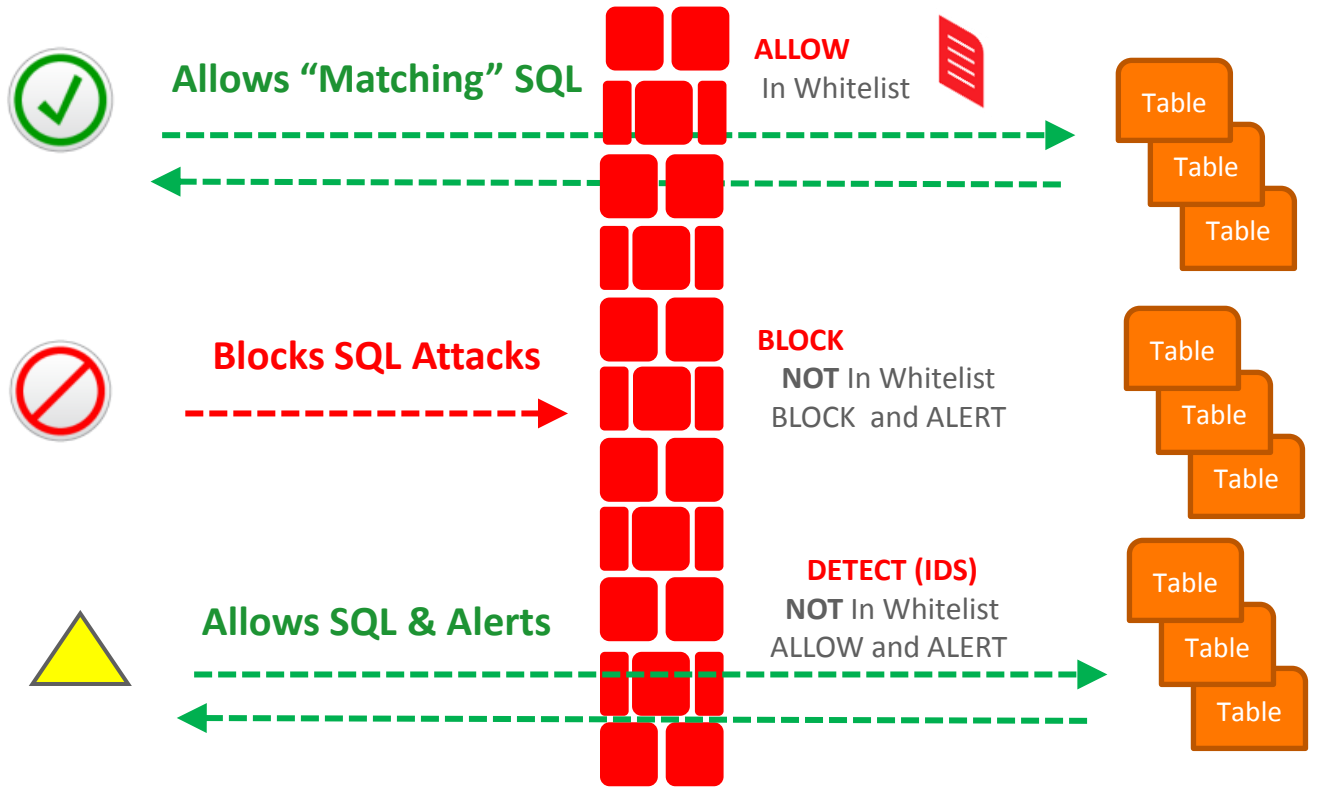


MySQL Enterprise Firewall: Overview

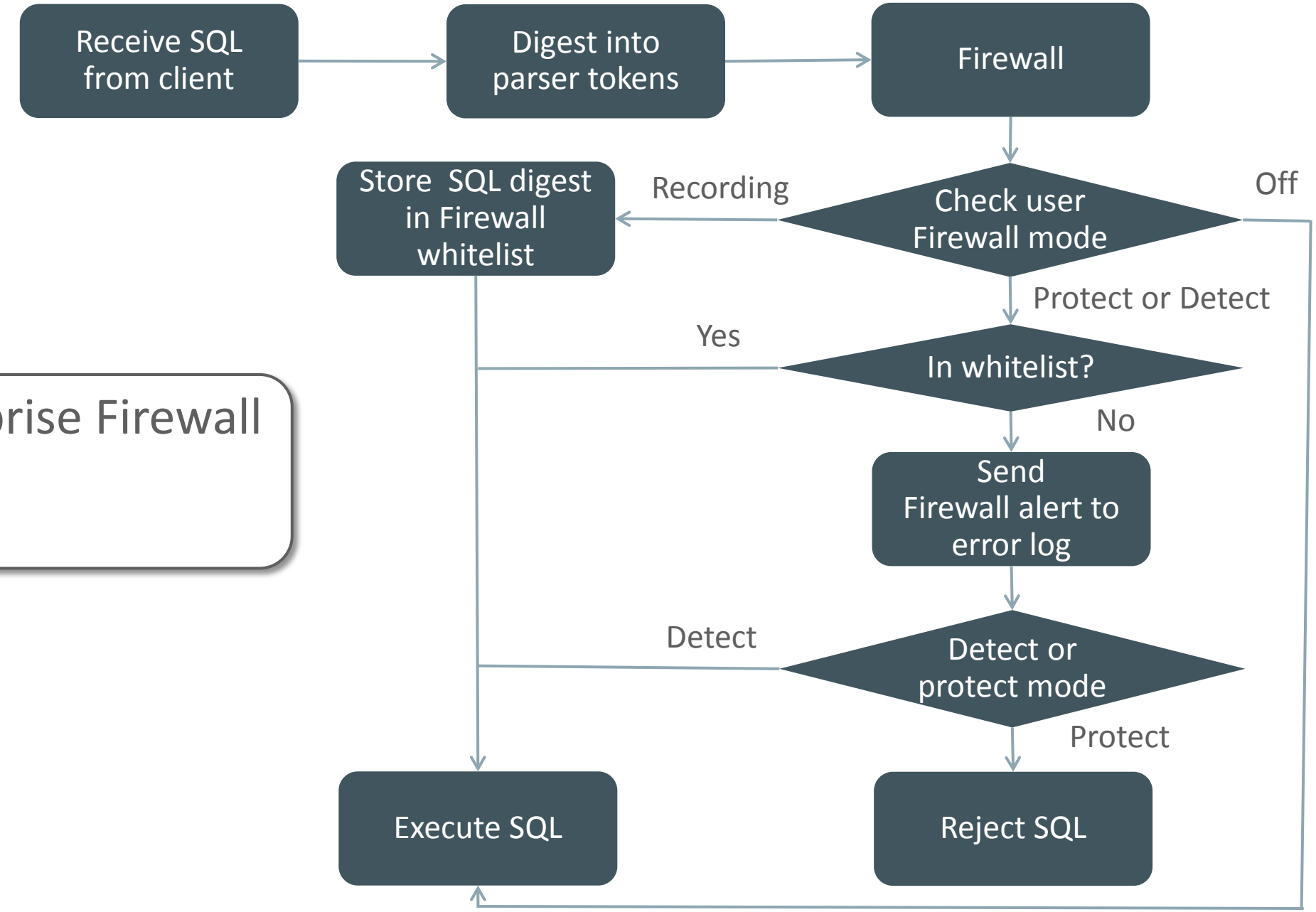


MySQL Enterprise Firewall: Operating Modes

1. ALLOW – Execute SQL
   - SQL Matches Whitelist
2. BLOCK – Block the request
   - Not in Whitelist
3. DETECT – Execute SQL & Alert
   - Not in Whitelist



MySQL Enterprise Firewall Workflow

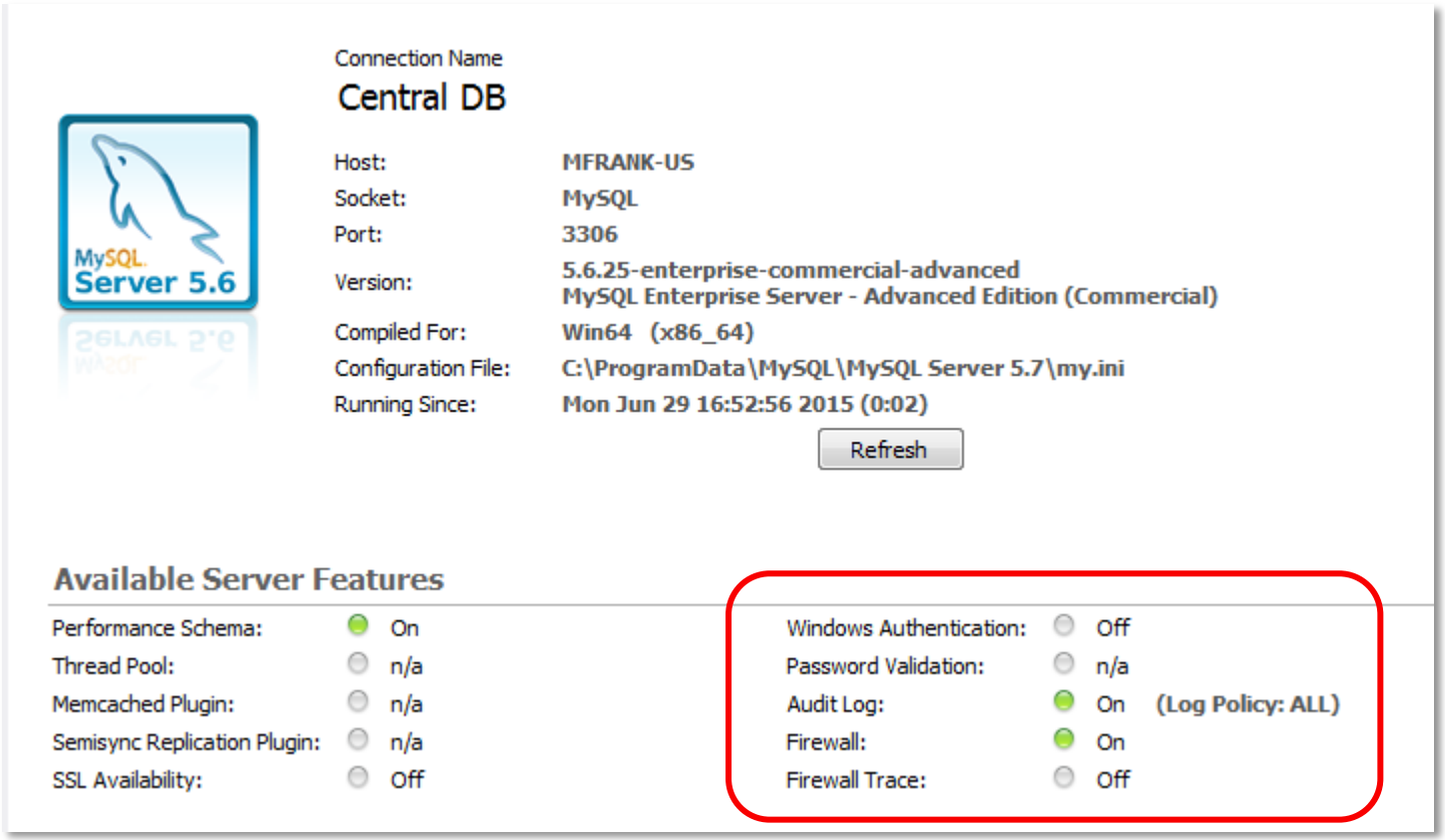


MySQL Enterprise Firewall Details

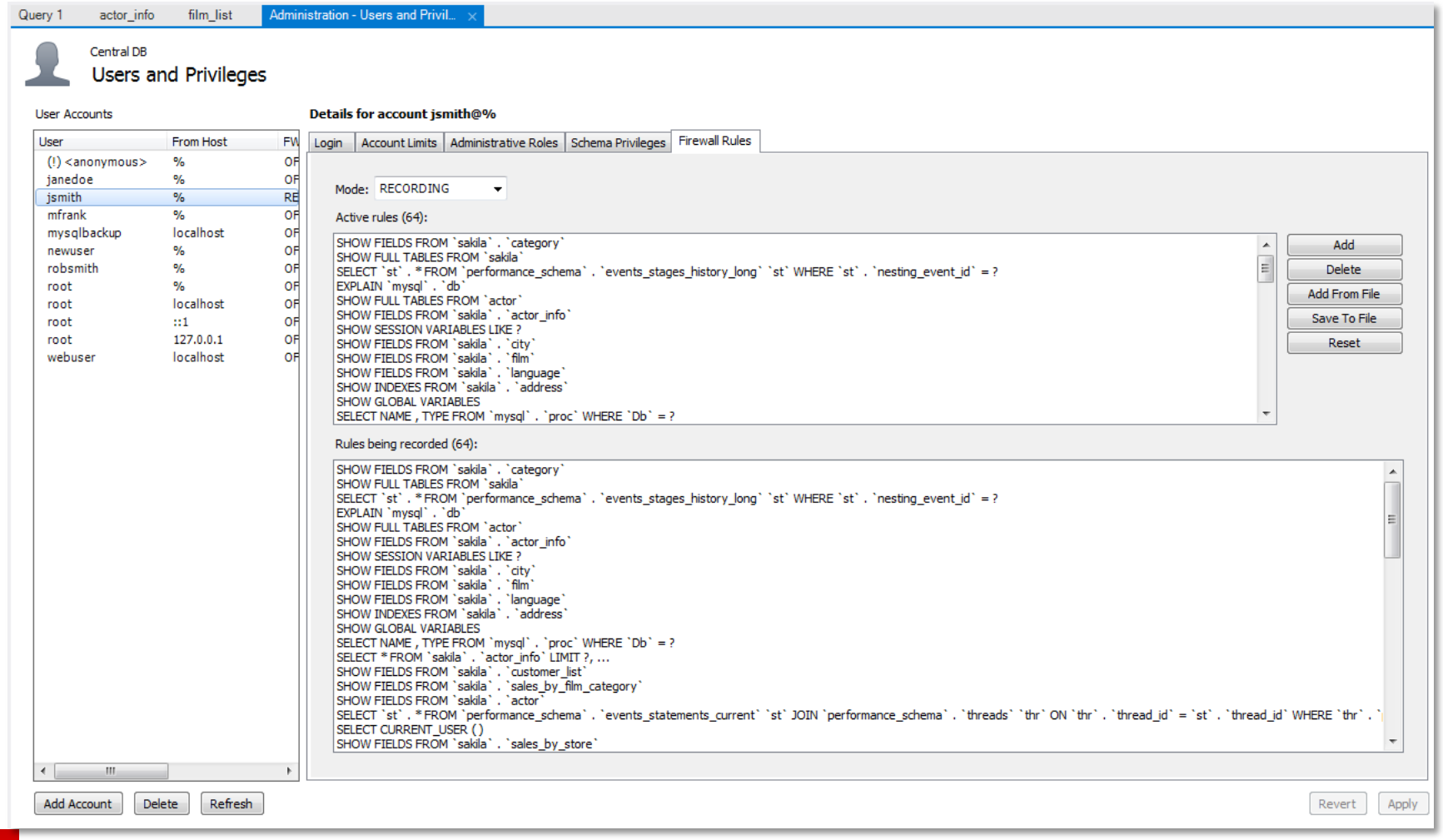
- Firewall operation is turned on at a per user level
- Per User States are
  - RECORDING
  - PROTECTING
  - DETECTING
  - OFF

```
call mysql.set_firewall_mode ('fwuser@localhost', 'RECORDING');
call mysql.set_firewall_mode ('fwuser@localhost', 'PROTECTING');
call mysql.set_firewall_mode ('fwuser@localhost', 'DETECTING');
call mysql.set_firewall_mode ('fwuser@localhost', 'OFF');
```

MySQL Workbench: Firewall Status



MySQL Enterprise Firewall: Per User Whitelists



MySQL Enterprise Firewall:
What happens when SQL is blocked in Protect Mode?

- The client application gets an ERROR

```
mysql> SELECT first_name, last_name FROM customer WHERE customer_id = 1 OR TRUE;
ERROR 1045 (28000): Statement was blocked by Firewall
mysql> SHOW DATABASES;
ERROR 1045 (28000): Statement was blocked by Firewall
mysql> TRUNCATE TABLE mysql.user;
ERROR 1045 (28000): Statement was blocked by Firewall
```

- Reported to the Error Log
- Increment Counter

MySQL Enterprise Firewall: Monitoring

Firewall Status Counters

```
mysql> SHOW GLOBAL STATUS LIKE 'Firewall%';
+------------------------------+-------+
| Variable_name                | Value |
+------------------------------+-------+
| Firewall_access_denied       | 3     |
| Firewall_access_granted      | 2     |
| Firewall_access_suspicious   | 1     |
| Firewall_cached_entries      | 4     |
+------------------------------+-------+
```

MySQL Enterprise Firewall: Whitelist Example

- `mysql> SELECT userhost, substr(rule,1,80) FROM mysql.firewall_whitelist WHERE userhost= 'wpuser@localhost';`

```
+------------------+--------------------------------------------------------------------------------+
| userhost         | substr(rule,1,80)                                                              |
+------------------+--------------------------------------------------------------------------------+
| wpuser@localhost | SELECT * FROM `wp_posts` WHERE `ID` = ? LIMIT ?                                |
| wpuser@localhost | SELECT `option_value` FROM `wp_options` WHERE `option_name` = ? LIMIT ?        |
| wpuser@localhost | SELECT `wp_posts` . * FROM `wp_posts` WHERE ? = ? AND `wp_posts` . `ID` = ? AND  |
...
| wpuser@localhost | UPDATE `wp_posts` SET `comment_count` = ? WHERE `ID` = ?                       |
| wpuser@localhost | SELECT `t` . * , `tt` . * FROM `wp_terms` AS `t` INNER JOIN `wp_term_taxonomy` A |
| wpuser@localhost | SELECT `t` . * , `tt` . * FROM `wp_terms` AS `t` INNER JOIN `wp_term_taxonomy` A |
+------------------+--------------------------------------------------------------------------------+
```

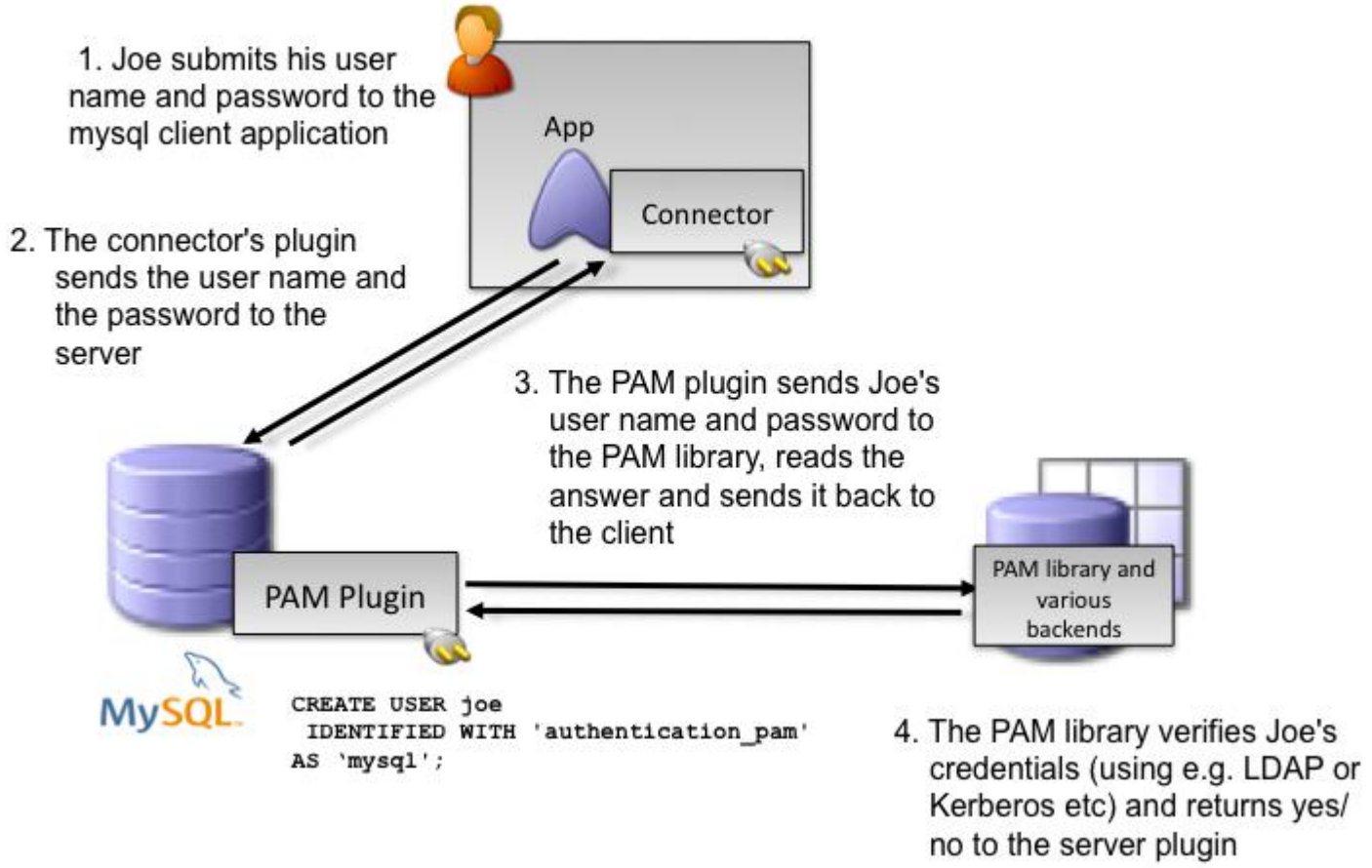
MySQL Enterprise Authentication

Integrates MySQL with existing security infrastructures

- Integrate with Centralized Authentication Infrastructure
  - Centralized Account Management
  - Password Policy Management
  - Groups & Roles
- PAM (Pluggable Authentication Modules)
  - Standard interface (Unix, LDAP, Kerberos, others)
  - Windows
    - Access native Windows service - Use to Authenticate users using Windows Active Directory or to a native host

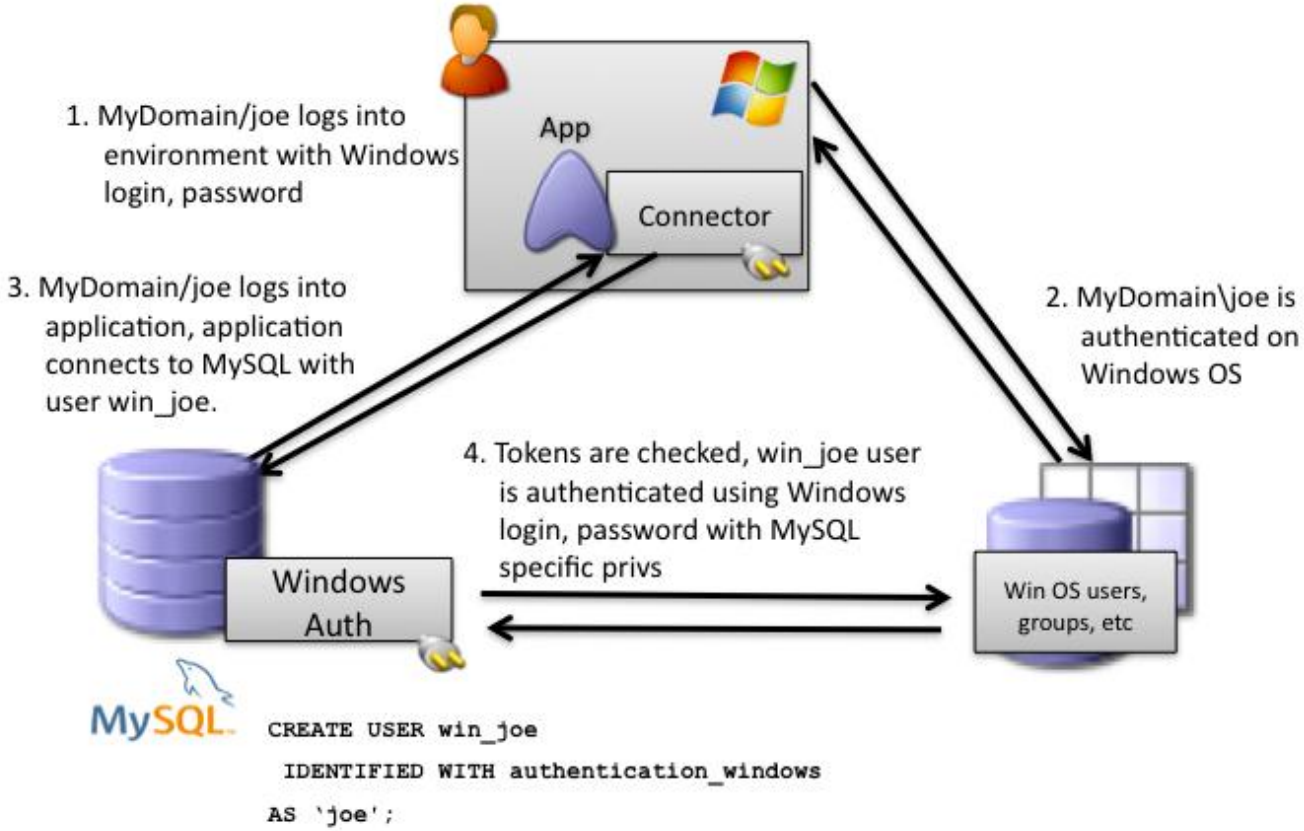
MySQL Enterprise Authentication: PAM

- Standard Interface
  - LDAP
  - Unix/Linux
- Proxy Users



MySQL Enterprise Authentication: Windows

- Windows Active Directory
- Windows Native Services

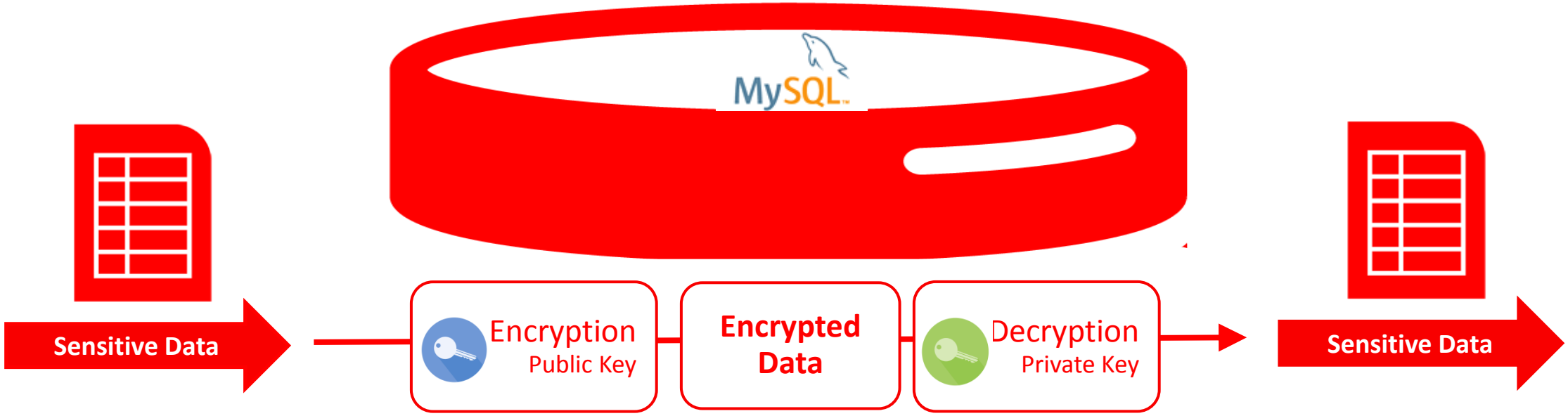


MySQL Enterprise Encryption

- MySQL encryption functions
  - Symmetric encryption AES256 (All Editions)
  - Public-key / asymmetric cryptography – RSA
- Key management functions
  - Generate public and private keys
  - Key exchange methods: DH
- Sign and verify data functions
  - Cryptographic hashing for digital signing, verification, & validation – RSA,DSA

MySQL Enterprise Encryption

Encryption/Decryption within MySQL

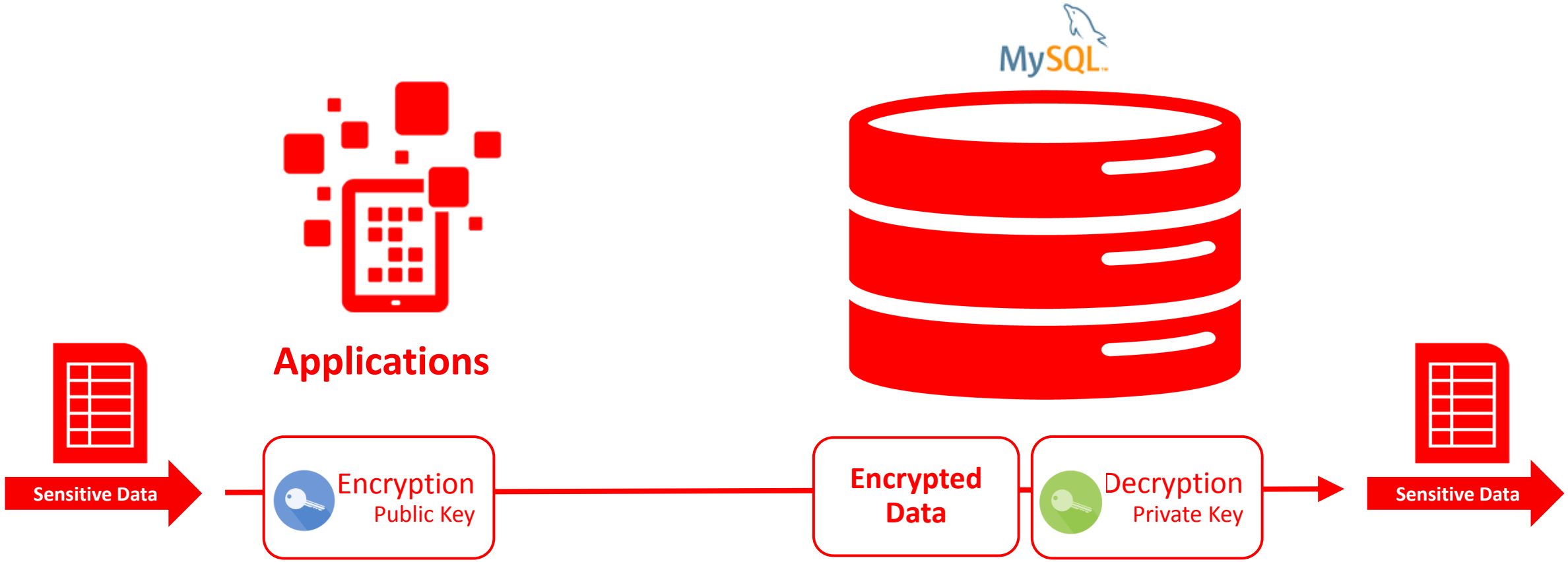


Private / Public Key Pairs

- Generate using MySQL Enterprise Encryption Functions
- Use externally generated (e.g. OpenSSL)

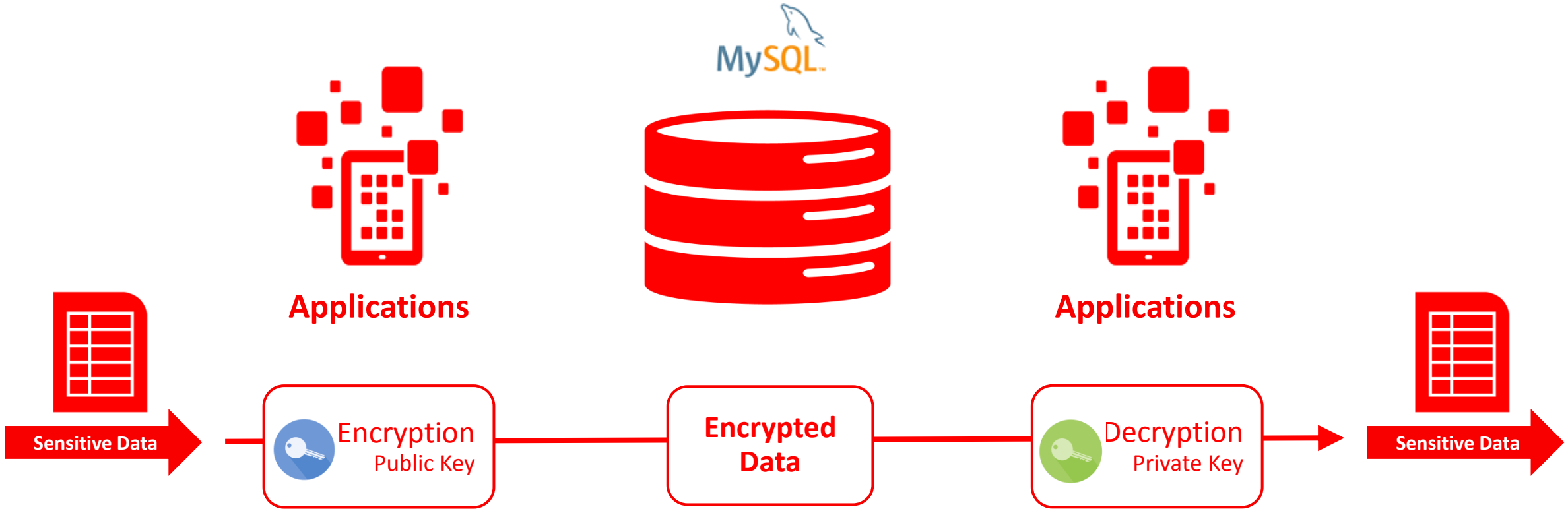
MySQL Enterprise Encryption

App Encrypts/MySQL Decrypts



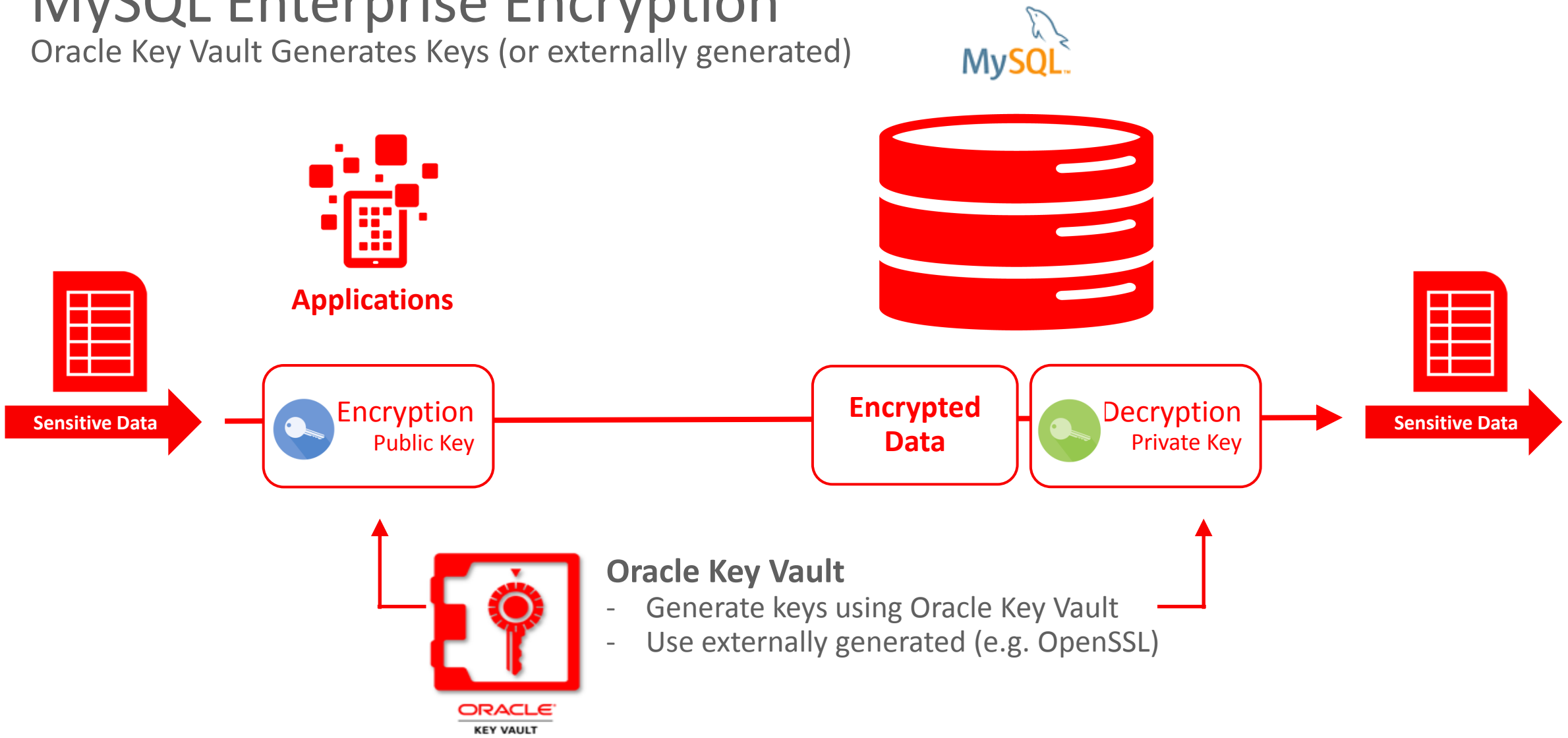
MySQL Enterprise Encryption

App Encrypts / MySQL Stores / MySQL Decrypts



MySQL Enterprise Encryption

Oracle Key Vault Generates Keys (or externally generated)



Oracle Key Vault

- Generate keys using Oracle Key Vault
- Use externally generated (e.g. OpenSSL)

ORACLE

MySQL Enterprise Audit

- Out-of-the-box logging of connections, logins, and query
- User defined policies for filtering, and log rotation
- Dynamically enabled, disabled: no server restart
- XML-based audit stream per Oracle Audit Vault spec

Adds regulatory compliance to MySQL applications (HIPAA, Sarbanes-Oxley, PCI, etc.)

MySQL Enterprise Audit

```
mysql> INSTALL PLUGIN audit_log SONAME 'audit_log.so';

mysql> SHOW VARIABLES LIKE 'audit_log%';
+-------------------------------+---------------+
| audit_log_buffer_size         | 1048576       |
| audit_log_connection_policy   | ALL           |
| audit_log_current_session     | OFF           |
| audit_log_exclude_accounts    |               |
| audit_log_file                | audit.log     |
| audit_log_flush               | OFF           |
| audit_log_format              | NEW           |
| audit_log_include_accounts    |               |
| audit_log_policy              | ALL           |
| audit_log_rotate_on_size      | 0             |
| audit_log_statement_policy    | ALL           |
| audit_log_strategy            | ASYNCHRONOUS  |
+-------------------------------+---------------+
```

1. DBA enables Audit plugin

```
shell> mysql -h joeshost -u joe -p
Enter password: ********

mysql> SELECT * FROM joes_table;
+---------------+--------------+
| FIRST_NAME    | LAST_NAME    |
+---------------+--------------+
| Joe           | User         |
+---------------+--------------+
```

2. User Joe connects and runs a query

3. Joe's connection & query logged

```
<?xml version="1.0" encoding="UTF-8"?>
<AUDIT>
  <AUDIT_RECORD
    TIMESTAMP="2012-08-02T14:52:12"
    NAME="Audit"
    SERVER_ID="1"
    VERSION="1"
    STARTUP_OPTIONS="--port=3306"
    OS_VERSION="i686-Linux"
    MYSQL_VERSION="5.5.28-debug-log"/>
  <AUDIT_RECORD
    TIMESTAMP="2012-08-02T14:52:41"
    NAME="Connect"
    CONNECTION_ID="1"
    STATUS="0"
    USER="joe"
    PRIV_USER="root"
    OS_LOGIN=""
    PROXY_USER=""
    HOST="SERVER1"
    IP="127.0.0.1"
    DB="joes_db"/>
  <AUDIT_RECORD
    TIMESTAMP="2012-08-02T14:53:45"
    NAME="Query"
    CONNECTION_ID="1"
    STATUS="0"
    SQLTEXT="SELECT * FROM joes_table;"/>
</AUDIT>
```

MySQL Enterprise Backup

- Online Backup for InnoDB (scriptable interface)
- Full, Incremental, Partial Backups (with compression)
- Strong Encryption (AES 256)
- Point in Time, Full, Partial Recovery options
- Metadata on status, progress, history
- Scales – High Performance/Unlimited Database Size
- Windows, Linux, Unix
- Certified with Oracle Secure Backup, NetBackup, Tivoli, others

MySQL Enterprise Oracle Certifications

- Oracle Enterprise Manager for MySQL
- Oracle Linux (w/DRBD stack)
- Oracle VM
- Oracle Solaris
- Oracle Solaris Clustering
- Oracle Clusterware
- Oracle Audit Vault and Database Firewall
- Oracle Secure Backup
- Oracle Fusion Middleware
- Oracle GoldenGate
- My Oracle Support

MySQL integrates into your Oracle environment

ORACLE

Oracle Audit Vault and Database Firewall

- Oracle DB Firewall
  - Oracle, MySQL, SQL Server, IBM DB2, Sybase
  - Activity Monitoring & Logging
  - White List, Black List, Exception List
- Audit Vault
  - Built-in Compliance Reports
  - External storage for audit archive


ORACLE®